Claims:

1. A handheld network connection created with at least two storage media in pocket format, with software for communication of data packets between at least two network access blockages of the type of at least one of a firewall, socks, IP-filter and proxy,

5   comprising:

each said storage media having an interface to a host computer in said networks, and which through software establishes communication with said host computer within said networks by utilizing said host computers temporary catalogues which provides access to said host computer without disturbing its file structure;

10   a crypto-daemon which comprises a connecting methodic testing to establish a tunneling to an external central server regarding the type of the allowable data packets for communication towards the existing type of access blockage, said crypto-daemon establishing said tunneling towards said external central server passing said access blockage through a test establishment of a communication with said access blockage, said

15   connecting methodic adapting to the wanted type of data packets by repeatedly questioning said access blockage for the allowable type of data packages until the correct type is encountered by remembering and repeatedly disregarding wrong questionings, and at the correct questioning changing the structure of the data package to the wanted structure for the specific port at hand for a communication; and

20   whereby an external network is established through said external central server outside said networks for simultaneous communication through at least two storage media and their software, said tunneling through said access blockage being provided without trespassing said networks per se, conveying towards said access blockage unrestricted capacity for said communication of data packets.

25   2. A network connection according to claim 1, wherein said methodic addresses the following software expressed in pseudo code while accessing a determined port:

```
check if proxy is to be utilized
If "OK"
    Test HTTP-proxy
30      If "OK"
        Connect through proxy
    Else
        Test SOCKS4-proxy
        If "OK"
35          Connect through SOCKS4-proxy
    Else
        Test SOCKS5-proxy
```

```
            If "OK"
                Connect through SOCKS5-proxy
        Else
            Test direct connection
                If "OK"
                    Provide direct connection
                Else
                    Direct connection failure
        Else
            Test direct connection
                If "OK"
                    Provide direct connection
                Else
                    Connection failure or test new port.
```

3. A network connection according to claim 1, wherein said methodic comprising for a future generation of proxy/firewall, only letting through granted traffic is overruled by hiding transmitted data through a dummy HTML page with said data masked.

4. A network connection according to claim 1, wherein accessible files through said host computer are fetched and encoded in the host computer temporary file catalogue, said files being stored encoded on the external central server, having a determined access profile allowing at least reading of said file but not copying from a computer outside the network with a connected host computer, thus allowing display of files outside said network.

5. A network connection according to claim 1, wherein said media allows its user to freely move in a host network and to communicate externally through said external central server with other users of the media through said tunneling.

6. A network connection according to claim 1, wherein said media software comprises IP-telephony, said user of the media from a computerized device of his choice in a network of his choice establishing spontaneous IP-telephony through said central server.

7. A network connection according to claim 1, wherein a creation of at least one of a radio channel and a film channel with other users in said external network is enabled by said media software, comprising streaming media, said users thus being able to consume music and film.

8. A network connection according to claim 1, wherein said media software comprises version handling, thus making possible to recreate earlier versions of files by saving changes in a separate memory in said external central server, being switched on/off through a server switch on the request of a user.

9. A network connection according to claim 1, wherein said media software enables multiple users of it to process a common text file in real time through said external central server.

10. A method for a handheld network connection created with at least two

5   storage media in pocket format, with software for communication of data packets between at least two network access blockages of the type of at least one of a firewall, socks, IP-filter and proxy, comprising the steps of:

each said storage media having an interface to a host computer in said networks, and which through software establishes communication with said host computer

10   within said networks by utilizing said host computers temporary catalogues which provides access to said host computer without disturbing its file structure;

having an access methodic comprised in a crypto-daemon testing to establish a tunneling to an external central server regarding the type of the allowable data packets for communication towards the existing type of access blockage, said crypto-daemon

15   establishing said tunneling towards said external central server passing said access blockage through a test establishment of a communication with said access blockage, said connecting methodic adapting to the wanted type of data packets by repeatedly questioning said access blockage for the allowable type of data packages until the correct type is encountered by remembering and repeatedly disregarding wrong questionings, and at the

20   correct questioning changing the structure of the data package to the wanted structure for the specific port at hand for a communication; and

whereby an external network is established through said external central server outside said networks for simultaneous communication through at least two storage media and their software, said tunneling through said access blockage being provided without

25   trespassing said networks per se, conveying towards said access blockage unrestricted capacity for said communication of data packets.

11. A method according to claim 10, wherein said methodic addresses the following software expressed in pseudo code while accessing a determined port:

check if proxy is to be utilized

30   If "OK"

    Test HTTP-proxy

      If "OK"

      Connect through proxy

    Else

35   Test SOCKS4-proxy

      If "OK"

      Connect through SOCKS4-proxy

```
            Else
                Test SOCKS5-proxy
                If "OK"
                    Connect through SOCKS5-proxy
5           Else
                Test direct connection
                If "OK"
                    Provide direct connection
                Else
10                  Direct connection failure
            Else
                Test direct connection
                    If "OK"
                        Provide direct connection
15                  Else
                        Connection failure or test new port.
```

12. A method according to claim 10, wherein said methodic comprising for a future generation of proxy/firewall, only letting through granted traffic is overruled by hiding transmitted data through a dummy HTML page with said data masked.

20   13. A method according to claim 10, wherein accessible files through said host computer are fetched and encoded in the host computer temporary file catalogue, said files being stored encoded on the external central server, having a determined access profile allowing at least reading of said file but not copying from a computer outside the network with a connected host computer, thus allowing display of files outside said network.

25   14. A method according to claim 10, wherein said media allows its user to freely move in a host network and to communicate externally through said external central server with other users of the media through said tunneling.

15. A method according to claim 10, wherein said media software comprises IP-telephony, said user of the media from a computerized device of his choice in a network of
30   his choice establishing spontaneous IP-telephony through said central server.

16. A method according to claim 10, creating at least one of a radio channel and a film channel together with other users in said external network by said media software, comprising streaming media, said users thus being able to consume music and film.

17. A method according to claim 10, wherein said media software comprises
35   version handling, thus making possible to recreate earlier versions of files by saving changes in a separate memory in said external central server, being switched on/off through a server switch on the request of a user.

18. A method according to claim 10, wherein said media software enables multiple users of it, to process a common text file in real time through said external central server.